REMARKS

The Examiner objected to the specification, in relation to claims 13-18. Since claims 13-18 have been cancelled, the objection to claims 13-18 is moot.

The Examiner rejected claims 13-18 under 35 U.S.C. §112, first paragraph. Since claims 13-18 have been cancelled, the rejection of claims 13-18 under 35 U.S.C. §112, first paragraph is moot.

The Examiner rejected claims 1-2, 5 and 8-10 under 35 U.S.C. §103(a) as allegedly being unpatentable over Freivald et al. (US Patent Number 6,012,087), and further in view of Shanklin et al. (US Patent Number 6,487,666), as evidenced by Chari et al. (US Patent Number 6,425,006).

The Examiner rejected claims 13-18 under 35 U.S.C. §103(a) as being allegedly unpatentable over the combination of Freivald and Shanklin. Since claims 13-18 have been cancelled, the rejection of claims 13-18 under 35 U.S.C. §103(a) is moot.

The Examiner rejected claims 3, 6 and 11 under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Freivald and Shanklin as applied to claims 2, 5 and 10 above respectively, and further in view of Lunt (Detecting Intruders in Computer Systems).

The Examiner rejected claims 4, 7 and 12 under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Freivald and Shanklin as applied to claims 2, 5 and 10 above respectively, and further in view of Martin et al. (US Patent Number 6,772,349).

Applicants respectfully traverse the §112 and §103 rejections with the following arguments.

35 U.S.C. §103(a): Claims 1-2, 5 and 8-10

The Examiner rejected claims 1-2, 5 and 8-10 under 35 U.S.C. §103(a) as allegedly being unpatentable over Freivald et al. (US Patent Number 6,012,087), and further in view of Shanklin et al. (US Patent Number 6,487,666), as evidenced by Chari et al. (US Patent Number 6,425,006).

Since claims 1-2 and 8-9 have been cancelled, the rejection of claims 1-2 and 8-9 under 35 U.S.C. §103(a) is moot.

Applicants respectfully contend that claims 5 and 10 not unpatentable over Freivald, and further in view of Shanklin, as evidenced by Chari, because Freivald, and further in view of Shanklin, as evidenced by Chari does not teach or suggest each and every feature of claims 1-2, 5 and 8-10 . For example, Freivald, and further in view of Shanklin, as evidenced by Chari does not teach or suggest the feature: "monitoring, by the intrusion detection system, for occurrence of a signature event that is indicative of a denial of service attack on a protected device, said denial of service attack attempting to impede operation of the protected device".

In addition, Applicants respectfully contend that the Examiner's argument for modifying Freivald by the alleged teaching of Shanklin is not persuasive, The Examiner argues: "Shanklin teaches a network intrusion detection system in which events are detected based on the signatures of the events (See Shanklin Abstract) and alerts are sent to the system manager (See Shanklin Col. 3 Lines 13-16), but Shanklin failed to disclose squelching the alerts once a certain alert generation threshold was reached.... It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the network intrusion detection system of Shanklin in the alert squelching system of Freivald, by utilizing the squelching system to lower the alert

generation rate of the intrusion detection system."

In response, Applicants maintain that the primary reference Freivald discloses an invention that is totally unrelated to an intrusion detection system for "monitoring ... occurrence of a signature event that is indicative of a denial of service attack on a protected device, said denial of service attack attempting to impede operation of the protected device". Therefore, it is not obvious to modify Freivald to incorporate the alleged teaching of Freivald.

In addition, Freivald, and further in view of Shanklin, as evidenced by Chari does not teach or suggest the feature: "when the value of the signature event counter exceeds the signature threshold quantity, generating an alert, recording a time of generating the alert in a **log**, determining from contents of the **log** a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold" (emphasis added).

The Examiner argues that "Freivald disclosed ...recording the time of the alarm in a log (See Freivald Col. 3 Lines 18-20, and Col. 7 Lines 39-41), using the log to determine the alert generation rate (See Freivald Col. 13 Lines 11-15)".

In response, Applicants maintain that the Examiner's citations in Freivald do not teach or suggest said feature of claims 5 and 10, because a log is not disclosed in the Examiner's citations in Freivald, and a log is certainly not disclosed in Freivald to determine a present alert generation rate.

Based on the preceding arguments, Applicants respectfully maintain that claims 5 and 10 are not unpatentable over Freivald, and further in view of Shanklin, as evidenced by Chari, and that claims 5 and 10 are in condition for allowance.

35 U.S.C. §103(a): Claims 3, 6, and 11

The Examiner rejected claims 3, 6 and 11 under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Freivald and Shanklin, and further in view of Lunt (Detecting Intruders in Computer Systems).

Since claim 3 has been cancelled, the rejection of claim 3 under 35 U.S.C. §103(a) is moot.

Since claim 6 depends from claim 5, which Applicants have argued *supra* to not be unpatentable over Freivald, and further in view of Shanklin, Applicants maintain that claim 6 is not unpatentable over the combination of Freivald and Shanklin and further in view of Lunt.

Since claim 11 depends from claim 10, which Applicants have argued *supra* to not be unpatentable over Freivald, and further in view of Shanklin, Applicants maintain that claim 11 is not unpatentable over the combination of Freivald and Shanklin and further in view of Lunt.

35 U.S.C. §103(a): Claims 4, 7, and 21

The Examiner rejected claims 4, 7 and 12 under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Freivald and Shanklin, and further in view of Martin et al. (US Patent Number 6,772,349).

Since claim 4 has been cancelled, the rejection of claim 4 under 35 U.S.C. §103(a) is moot.

Since claim 7 depends from claim 5, which Applicants have argued *supra* to not be unpatentable over Freivald, and further in view of Shanklin, Applicants maintain that claim 7 is not unpatentable over the combination of Freivald and Shanklin and further in view of Martin.

Since claim 12 depends from claim 10, which Applicants have argued *supra* to not be unpatentable over Freivald, and further in view of Shanklin, Applicants maintain that claim 12 is not unpatentable over the combination of Freivald and Shanklin and further in view of Martin.

CONCLUSION

Based on the preceding arguments, Applicants respectfully believe that all pending claims and the entire application meet the acceptance criteria for allowance and therefore request favorable action. If the Examiner believes that anything further would be helpful to place the application in better condition for allowance, Applicants invites the Examiner to contact Applicants' representative at the telephone number listed below. The Director is hereby authorized to charge and/or credit Deposit Account No. 09-0457.

Date: 06/20/2005

Jack P. Friedman
Registration No. 44,688

Schmeiser, Olsen & Watts
3 Lear Jet Lane, Suite 201
Latham, New York 12110
(518) 220-1850